

Attached Document #1

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MALIBU MEDIA, LLC,
Plaintiff,

CASE No. 2:12-CV-02084

v.

JOHN DOES 1-14,
Defendants.

_____ /

**DECLARATION TO REFUTE INFORMATION PROVIDED BY PLAINTIFF'S
COUNSEL, CHRISTOPHER FIORE, 14 MAY 2012 HEARING**

I, an anonymous John Doe, do hereby declare:

1. I'm over 18 years of age and competent to make this declaration.
2. I have personal knowledge of the facts in this declaration and the information provided by Plaintiff's counsel, Christopher Fiore, on 14 May 12 (Document #6), during the motion hearing for cases 2:12-CV-02078, 2:12-CV-02084, and 2:12-CV-02088 (Malibu Media LLC is the Plaintiff for these cases), in support of Plaintiff's motion for leave to take discovery prior to Rule 26(f) conference.
3. I have also sent six previous declarations (October 2011 – January 2012) for copyright infringement cases for various courts: Eastern District of Virginia (Richmond Division), *3:11-cv-00531-JAG (Patrick Collins v. Does 1-58)*, *3:11-cv-00469-JAG (K-Beech v. Does 1-85)*, District of Arizona, *2:11-cv-01602-GMS (Patrick Collins v. Does 1-54)*, the Northern District of Florida, *4:11-CV-00584 (Digital Sin, Inc., v. Does 1-145)*, Northern District of Illinois, *1:11-CV-09064 (Pacific Century International v. Does 1-31)*, and the District of Columbia, *1:12-cv-00048 (AF Holdings, LLC, v. Does 1-1058)*, refuting various Plaintiff

being abused by Plaintiffs and copyright infringement lawyers who follow this business model. Some of the Doe defendants I have interacted with have been pressured to settle with clients of Mr. Fiore for cases filed in the Eastern District of Pennsylvania.

6. I hope my declaration will aid the Court in understanding the questionable practices of Plaintiff, copyright infringement lawyers in general, and correcting the information Mr. Fiore presented the court during the 14 May 12, hearing. The anonymous nature of this declaration does not detract from its logic, truthfulness, and will only aid in the understanding of these technically complex types of cases. I thank the court for indulging this John Doe.

7. BitTorrent

BitTorrent is a computer program and protocol (system of rules) for sharing large files across the Internet. BitTorrent is part of a group of file sharing applications, known as peer-to-peer (P2P). BitTorrent is completely legal and only a tool in which the individual user decides how it is used. The company was founded in 2004 and their main office is located in San Francisco, CA. Details concerning BitTorrent can be found at www.bittorrent.com. BitTorrent can and is used by personnel engaged in illegal file sharing, to include Plaintiff's movies. It is also used to legally distribute various files, to include software, music, ebooks, and movies. The BitTorrent Company and the various versions of its file sharing software are not hidden in some basement in Eastern Europe or Asia as Mr. Fiore suggests. This statement makes it seem that Mr. Fiore has very little knowledge on the software that plays a central part in these copyright infringement cases he is filing.

8. Wireless Networking

Mr. Fiore claims all the Doe defendants (public IP addresses) had to take active steps to install the BitTorrent software on their computers and was not an accidental matter.

Mr. Fiore omits to tell the court the public IP address Plaintiff's agents recorded does not necessarily correlate to the BitTorrent software being installed on any computer belonging to Doe defendants. The public IP address Plaintiff provided the court only correlates to the immediate location of the Internet service and who pays the Internet Service Provider (ISP). This is due to the fact that a majority of homes and small businesses today use a Wireless Firewall/Router (WFR) to share the Internet connection to systems at their location. The WFR allows multiple wired and wireless connections from computers (some possibility unauthorized); all using the same Public IP address Plaintiff has collected (Exhibit A). As the wireless signal of the WFR commonly extends outside the residence, it is not unusual for unauthorized systems to connect to it. Some ISP subscribers (Doe defendants) may have run their wireless Internet connection open (no password required), so anyone could have connected to it and downloaded Plaintiff's movie. Even if an ISP subscriber secures the wireless Internet connection with a password, there are various vulnerabilities that could be exploited to gain access to it.

Possible claims of negligence on the part of Doe defendants in not securing an Internet connection or by not monitoring what occurs on it are baseless. There is no legal duty or contractual obligation between the defendants and Plaintiff to require such action. On 30 Jan 12, Judge David Ezra, stated the following concerning negligence claims in copyright infringement case 1:11-cv-00262, Liberty Media Holdings, LLC, v. Hawaii members of swarm...,

The Court concludes that the allegations in the FAC are not sufficient to state a claim for negligence for a couple reasons. First, nowhere in the FAC does Plaintiff assert any specific legal duty in connection with its negligence claim. Further, Plaintiff has not cited, nor has the Court found, any case law with analogous facts from which the Court could conclude that the Defendants owed Plaintiff a general duty to secure their internet connection. Second, even assuming

Plaintiff had alleged a cognizable duty, the FAC fails to allege any facts demonstrating how Plaintiff breached that duty. Plaintiff's Memorandum in Opposition to the instant Motion highlights the purported risks associated with failing to password-protect one's wireless network. However, Plaintiff does not allege in the FAC that any of the individual Defendants failed to password-protect his/her wireless network or otherwise monitor the use of his/her computer by others. The bare assertion that they "failed to adequately secure their Internet access" is conclusory and unsupported by specific factual allegations regarding the individual Defendants. Therefore, it is not entitled to an assumption of truth for purposes of ruling on the instant Motion. (*1:11-cv-00262-DAE-RLP, Document #66, Order: (1) Granting in Part and Denying in Part Defendant Hatcher's Motion to Dismiss, (2) Granting Plaintiff's Leave to Amend, and (3) Vacating the Hearing, Page 13*)

The WFR provides each system connected to it an "internal" IP address that no one outside the home network will ever see (Exhibit A). The unauthorized use of a defendant's Internet connection is sometimes unwittingly done by a neighbor, but has also been done by malicious third-parties wishing to avoid detection of illegal activity or to implicate a defendant in a crime. Due to the technical nature of the WFR, most users set-up the device and never touch it again unless there is a problem. Most users will never know their Internet connection was illegally used by third parties unless they receive some notification. One such common notification is the Digital Millennium Copyright Act (DMCA) take-down notice from a copyright content owner. Note: most pornography copyright content owners do not issue DMCA take-down notices to ISPs and their customers (Doe defendants). Due to the very limited network logging ability of most WFR, by the time the ISP notifies the subscriber of a legal action (such as this case), any WFR logs showing possible third-party users are long gone. If DMCA take-down notices were immediately issued to the ISPs and Doe defendants, there is a better chance of the WFR having relevant logs.

Two 2011 Federal court filings from defendants in a similar California copyright infringement case (*3:11-cv-02766-MEJ, Northern District of CA, Patrick Collins v. Does 1-*

2590, Documents 22 and 52), show how weak the Public IP address is in identifying the actual copyright infringers.

In document 22 (3:11-cv-02766-MEJ), Bobbie Thomas (ISP subscriber), Richmond, CA, tells the court she is a disabled female who lives with her adult daughter and several in-home care providers. The residence (location of the Public IP address) is a three-story building in which her daughter runs a child day care business for 12-hours a day. In the first floor common area, Mrs. Thomas' personal computer and Internet connection were open and available for any of the residents or anyone with access to use.

In document 52 (3:11-cv-02766-MEJ), Steve Buchanan (ISP subscriber), Phoenix, AZ, tells the court that unknown personnel were abusing his Internet connection and his ISP had to help him re-secure his WFR. Mr. Buchanan enlisted the help of his ISP after receiving notification from his ISP that copyright protected movies were being shared via his public IP address. Mr. Buchanan eventually secured his WFR and determined that unknown personnel had also illegally accessed his wife's computer and prevented it from connecting to his network.

The unauthorized use of a home WFR led to one Buffalo, NY, family to being investigated for allegedly downloading child pornography. On 7 March 2011, US Immigration and Customs (ICE) agents executed a search warrant for child pornography based only on the subscriber information (Public IP address) they received from the ISP. ICE later determined that a next-door neighbor had used the Internet connection via the WFR.²

In July 2011, Barry Ardolf, Minnesota, was convicted of hacking a neighbors (Matt and Bethany Kostolnik) WFR, trying to frame them with child pornography, sexual

²http://www.huffingtonpost.com/2011/04/24/unsecured-wifi-child-pornography-innocent_n_852996.html, *Innocent Man Accused of Child Pornography After Neighbor Pirates His WiFi*, 24 Apr 11.

harassment, and even sending threatening emails to Vice President Joe Biden.³ Mr. Ardolf used freely available software and manuals to hack the Wired Equivalent Privacy (WEP) protecting the Kostolnik's WFR. Due to the threatening emails sent to the Vice President, the US Secret Service contacted Mr. Kostolnik based on the email and Public IP address. Mr. Kostolnik was eventually cleared of these allegations after it was determined Mr. Ardolf hacked their WFR. Mr. Ardolf was eventually sentenced to 18 years in prison (*case 0:10-cr-00159-DWF-FLN, USDC, District of Minnesota*).⁴

Examples of why the registered IP subscriber did not illegally download/share the copyright protected movie are:

- a. Home Wireless Internet access point run open (like at an airport or coffee bar) and abused by an unknown person.
- b. Guest at the residence abusing the Internet connection without the owner knowing.
- c. Neighbor connects (knowingly or unknowingly) to the network and the owner doesn't know of this activity.
- d. IP address is part of a group residence (roommates), apartment building, or small home business where a user (not the ISP subscriber) downloaded/shared copyright protected movie.
- e. Home system infected by a Trojan Horse malware program and controlled by unknown personnel.
- f. Unknown person hacks the Wireless security settings of the WFR to abuse the owners Internet connection.⁵

Without additional investigative steps, innocent personnel are bound to be implicated in infringement activity and pressured to pay a settlement to make the threat of a federal law suit go away. One earlier court noted the problem with only using the Public IP address to identify the alleged infringer:

³<http://www.networkworld.com/news/2011/07/13/11-wifi-hack.html>, "Depraved" Wi-Fi hacker gets 18 years in prison, 13 Jul 11.

⁴http://www.wired.com/images_blogs/threatlevel/2011/07/ardolfedssentencingmemo.pdf, Government's Position With Respect to Sentencing, 14 Jul 11.

⁵<http://www.kb.cert.org/vuls/id/723755>, WiFi Protected Setup (WPS) PIN brute force vulnerability, Vulnerability Note VU# 723755, 27 Dec 11

Comcast subscriber John Doe 1 could be an innocent parent whose internet access was abused by her minor child, while John Doe 2 might share a computer with a roommate who infringed Plaintiffs' works. John Does 3 through 203 could be thieves, just as Plaintiffs believe, inexcusably pilfering Plaintiffs' property and depriving them, and their artists, of the royalties they are rightly owed. . . . Wholesale litigation of these claims is inappropriate, at least with respect to a vast majority (if not all) of Defendants. *BMG Music v. Does 1-203*, No. Civ.A. 04-650, 2004 WL 953888, at *1 (E.D. Pa. Apr. 2, 2004) (severing lawsuit involving 203 defendants).

Without informing the court of these facts, it is irresponsible for Mr. Fiore to tell the court that ALL the defendants installed BitTorrent software and knowingly took part in the illegal download/sharing of a copyright protected movie just because Plaintiff recorded their public IP address.

9. Media Access Control (MAC) Address

The MAC address the ISPs have on record for Doe defendants is a type of serial number found on devices with a computer networking capability. Common networking enabled devices include computers, smart phones, video game systems, televisions, and DVD players. Many ISPs use the MAC address as a screening filter to limit access to their network to only the paying customers. Depending on the specific ISP, the MAC address recorded may be for the cable/DSL modem or the first network enabled device connected to the modem. If a Doe defendant only has one computer connected directly to the cable/DSL modem, then the ISP may record the MAC address for this device. As it is common today for personnel to first connect a WFR into the cable/DSL modem, the MAC address recorded by the ISP may be for this device. None of MAC addresses for the internal devices connected to the WFR (wired or wireless) are seen or recorded by the ISP or anyone else outside of the home network (Exhibit A). As previously stated, the logging ability of the WFR is very limited and the fact that Plaintiff waited so long to file this case, relevant logs are likely gone.

10. Determination of the Actual Infringer

Plaintiff has no intention of identifying the actual copyright infringers with this action. Plaintiff's goal is to obtain ISP subscriber information for the public IP addresses they recorded, issue settlement demands, and eventually dismiss the cases without naming or serving a single defendant. Plaintiff claims the public IP address shows the ISP subscriber is responsible for the infringement activity. As shown above, this logic is flawed and to truly determine the infringer, more investigative effort has to be accomplished. The history of copyright infringement law suits by pornography content owners shows the overwhelming majority of defendants are never named and served with a summons. On 24 Feb 2012, Prenda Law Inc., one of the main copyright infringement law firms in the U.S., stated the following.

Although our records indicate that we have filed suits against individual copyright infringement defendants, our records indicate no defendants have been served in the below listed cases. (*AF Holdings LLC, v. Does 1-135, case 5:11-cv-03336-LHK (NDCA)*, Document 43 (*Declaration of Charles Piehl*), Exhibit A, section 9.)

Note: the number of cases in the Prenda document was 118, with over 15,000 Doe defendants since 2010. Out of 15,000+ Doe defendants, none were named and served with a summons (as of 24 Feb 12). I'm confident that if asked to produce a similar document, Mr. Fiore's report would be very similar for the cases he has filed in the EDPA.

11. Order & Report & Recommendation, Case 2:11-cv-03995, Judge Gary Brown (EDNY)

The basis of the 14 May 12, hearing was to address concerns the court had with Plaintiff's cases, as raised by Judge Brown's 1 May 12, Order & Report & Recommendation (ORR), Case 2:11-cv-03995, Document 39, Eastern District of New York. It is shocking Mr. Fiore didn't know about this ORR, as it deals with his client directly and was seen as a major set-back to the current copyright infringement law suits in EDNY and highly relevant to all law firms pursuing

these cases.

The court's question to Mr. Fiore about placing all of these types of copyright infringement cases under one judge is a valid one. Mr. Fiore doesn't directly state they shouldn't be placed under one judge, but he infers it is likely his view. Mr. Fiore incorrectly tells the court that as these copyright infringement cases are all "different," they should not be consolidated under the same judge. The issue is not that all of the EDPA pornography copyright infringement law suits have different Plaintiffs, different movies, and different Doe defendants. The key issue is they are all the same type of pornography copyright infringement law suit. Here are the main reasons why the EDPA should consolidate them under one judge (or limited number).

- These cases can be highly technical and a good understanding of computers/networking and Internet file sharing is needed. Having to repeatedly educate judges new to this case type on the technical aspects is a waste of limited judicial resources.
- The consolidation will ensure a uniform response for Plaintiffs and Doe defendant motions and case management, independent of which court the case is assigned to.
- All of the complaints for these cases are for Copyright Infringement in accordance with Title 17, Section 101.
- All of the alleged infringed copyright protected content is adult pornography.
- All of the alleged copyright infringement occurred via Internet file sharing applications, primarily BitTorrent.
- All the Plaintiffs in these cases employ some sort of technical monitoring service to record the public IP address of alleged infringers.
- All cases deal with Doe defendants who are only identified by their public IP address.

- All Plaintiffs seek leave to serve third party subpoenas prior to a Rule 26(f) Conference. The third party is the ISP who has the contact information (name, address, telephone number, email) for the subscriber assigned the public IP address Plaintiff recorded.
- Many Doe defendants in these cases file motions to quash, dismiss, or sever, based on claims of improper joinder, improper jurisdiction, or lack of prima facie evidence.
- Once the contact information for the Doe defendants are obtained, Plaintiffs make settlement demands of thousands of dollars to make the fear of a law suit go away.
- For over 200,000 Doe defendants nation-wide since 2010, there have only been a handful of default judgments issued. Most Plaintiffs dismiss the cases against non-settling Doe defendants. The goal with these types of law suits is not to prevent copyright infringement, but to generate revenue on a repeatable basis.

In his ORR (case 2:11-cv-03995), Judge Brown correctly described the litigation practices of these cases as “Abusive.”

Our federal court system provides litigants with some of the finest tools available to assist in resolving disputes; the courts should not, however, permit those tools to be used as a bludgeon. As one court advised Patrick Collins Inc. in an earlier case, “while the courts favor settlements, filing one mass action in order to identify hundreds of doe defendants through pre-service discovery and facilitate mass settlement, is not what the joinder rules were established for.” *Patrick Collins, Inc. v. Does 1–3757*, 2011 U.S. Dist. LEXIS 128029, at *6–7 (N.D.Cal. Nov. 4, 2011).

After my personal information was released to my Plaintiff, I was repeatedly threatened with an individual law suit. I was told I was responsible and there was no defense. I was told that unless I settled, the case would drag on for a year or two, and it

would cost me thousands more dollars than settling. My Plaintiff eventually dismissed the case after keeping it open for more than a year. I was never named in any complaint and never received a summons, even after repeated calls and letters stating they were about to take such actions. On 1 December 2011, Judge Maria-Elena James, Northern District of California (*case # 3:11-cv-02766-MEJ, Patrick Collins v. Does 1-2590*), commented on this practice.

Since granting Plaintiff's request, a check of the Court's docket disclosed that no defendant has appeared and no proof of service has been filed. Further, the Court is aware that this case is but one of the many "mass copyright" cases to hit the dockets of federal district courts across the country in recent months. Like in this case, after filing the suit, the plaintiff seeks discovery from ISPs who possess subscriber information associated with each IP address. With the subscriber information in hand, the court is told, the plaintiff can proceed to name the defendants in the conventional manner and serve each defendant, so that the case may proceed to disposition. This disposition might take the form of settlement, summary judgment, or if necessary, trial. In most, if not all, of these cases, if the plaintiff is permitted the requested discovery, none of the Doe defendants are subsequently named in the cases; instead, the plaintiff's counsel sends settlement demand letters and the defendants are subsequently dismissed either by the Court or voluntarily by the plaintiff.

12. Conclusion

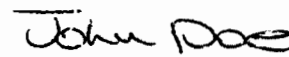
The copyright infringement of protected works, such as Plaintiff's, is a problem and the owners have the right to seek redress for it. Plaintiff's misuse of the court in seeking redress stems from the weak prima facie evidence collected (public IP address) coupled with abusive settlement practices. Plaintiffs commonly set the settlement fee for defendants at the point where it costs them more to fight than settle, regardless of guilt or innocence. The threat of possible financial ruin, family and friend embarrassment, a convenient settlement option, and non-disclosure agreement, make it easy for even innocent people to possibly accept paying the settlement fee. Plaintiff knows their evidence collections methods are not 100% effective at identifying the actual infringers. To admit this short coming risks the prof-

itability of this business model and future operations. The fact that a majority of Federal civil cases are settled before trial should not be the justification basis for allowing this activity to continue. Plaintiff and the growing number of copyright infringement lawyers are abusing the court for their financial gain. These cases and other like it in the EDPA (past, present, and future) will follow the standard course of action: (1) release of ISP subscriber information, (2) settlement demands made by Plaintiff, and (3) dismissal of the cases after settlements are collected from some defendants (Noting that no defendants will be named and served).

I thank the court for hearing this declaration.

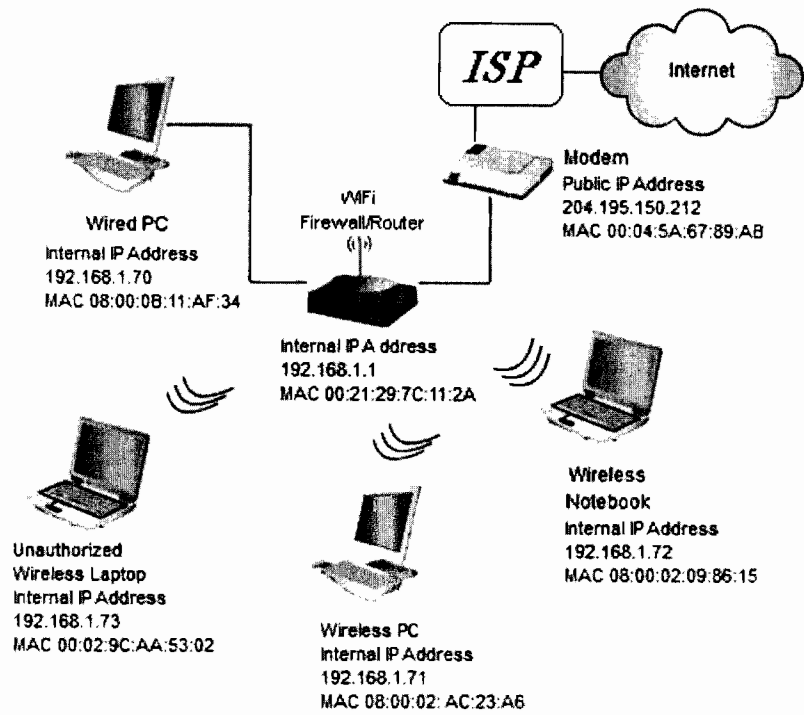
Dated: 5/31/2012

Respectfully submitted,

A handwritten signature in black ink that reads "John Doe". The signature is written in a cursive, slightly stylized font.

John Doe, AKA: DieTrollDie
Web site: <http://dietrolldie.com>
Doerayme2011@hotmail.com

Example of home network using a Wireless Firewall/Router



The following table is an example of a Dynamic Host Configuration Protocol (DHCP) host table maintained inside the Wireless Firewall Router. It shows the names, Internal IP address, MAC addresses, and IP address lease expiration time for systems that are connected to the network. Note: this example does not directly correspond to the network diagram above.

DHCP Active IP Table

DHCP Server IP Address: 192.168.1.1

Refresh

Client Host Name	IP Address	MAC Address	Expires	Delete
SipuraSPA	192.168.1.64	00:0E:0B:CD:C9:96	20:01:48	<input type="checkbox"/>
stephani-15edaa	192.168.1.65	00:0C:76:58:C4:0A	06:49:53	<input type="checkbox"/>
admin-kroni9y1B	192.168.1.66	00:08:02:FE:BB:22	23:43:47	<input type="checkbox"/>
lucas-be6n1j9k	192.168.1.69	00:20:ED:33:70:F4	13:12:54	<input type="checkbox"/>

Close